TRABAJO DE GRADO

PLAN DE CONCIENCIACIÓN SOBRE LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DE SALUD DEL SECTOR PÚBLICO DE BOGOTÁ.

FABIO MARTÍNEZ OSORIO.

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

TRABAJO DE GRADO

PLAN DE CONCIENCIACIÓN SOBRE LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DE SALUD DEL SECTOR PÚBLICO DE BOGOTÁ.

FABIO MARTÍNEZ OSORIO.

Trabajo de grado presentado para optar al título de Especialista en Seguridad de la Información

Docente

MSC ALFONSO LUQUE ROMERO
DOCENTE ESPECIALIZACIÓN

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE GRÁFICAS

LISTA DE IMAGENES

1. INTRODUCCIÓN

Durante los últimos años y según estudios realizados, se ha evidenciado el aumento de ataques informáticos que apuntan al sector salud - y no es de asombrarse – considerando la importancia y sensibilidad de los datos que se manejan, adicionando el tema de que en su mayoría los funcionarios que aquí trabajan son inexpertos en cuanto a temas de seguridad de la información; punto a favor de los delincuentes informáticos, quienes se han aprovechado de esta situación para poder ejecutar sus ataques de manera más fácil.

Este trabajo de grado tiene como finalidad detectar la falta de concienciación de los funcionarios de las entidades de salud del sector público de Bogotá respecto a temas de seguridad de la información, y en consecuencia generar un plan de concienciación que refleje la importancia de fomentar una cultura basada en buenas prácticas para ayudar a reducir los ataques informáticos a los cuales se encuentran expuestos y contribuir al cumplimiento de las políticas internas de estas organizaciones.

Para su desarrollo y con el fin de detectar esta falta de conciencia, se empleó el uso de una herramienta de autodiagnóstico disponible por el Instituto Nacional de Ciberseguridad (INCIBE)[1] y la aplicación de una encuesta diseñada por el autor, a un grupo de funcionarios de algunas instituciones de salud del sector público de Bogotá, y quienes por temas de confidencialidad solicitaron mantener el anonimato de su nombre y cargo desempeñado.

Posteriormente, se hizo una comparación entre los resultados obtenidos una vez aplicada la herramienta de autodiagnóstico y la encuesta, para identificar los temas sobre los cuales se hace necesario empezar a concienciar a los funcionarios del sector seleccionado.

Una vez identificados los temas sobre los cuales se hace necesario fomentar mejores prácticas y teniendo como base las recomendaciones incluidas en el Plan de capacitación, sensibilización y comunicación de la seguridad de la información generado por el MINTIC[2] y en la publicación especial NIST SP 800-50[3] se procedió

[1] INCIBE: El Instituto Nacional de Ciberseguridad es una empresa pública organizada como sociedad anónima estatal propiedad del Ministerio de Asuntos Económicos y Transformación Digital de España a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

[2] MINTIC: Ministerio de Tecnologías de la Información y las comunicaciones de Colombia.

[3] NIST 800-50: Creación de un programa de capacitación y concienciación sobre seguridad en tecnologías de la información.

a la elaboración del plan de concienciación dirigido a los funcionarios objeto de este estudio y el cual contiene la información necesaria para empezar a desarrollar el plan en las entidades de salud del sector público de Bogotá teniendo en cuenta sus recursos disponibles.

2. GENERALIDADES

I. LÍNEA DE INVESTIGACIÓN

La línea de investigación seleccionada para desarrollar este proyecto es: Software Inteligente y Convergencia Tecnológica.

II. PLANTEAMIENTO DEL PROBLEMA

A medida que la industria de la salud continúa su camino acelerado hacia el mantenimiento de registros digitales y médicos mediante el software de historia clínica y otras herramientas electrónicas, los hospitales, clínicas y prestadores e instalaciones de salud de todos los tamaños deben prepararse para la posibilidad muy real de ser golpeados por un ciberataque o cualquier tipo de amenaza que ponga en peligro los datos que se alojan en este tipo de aplicaciones, razón por la que deben armarse en infraestructura robusta y una cultura de seguridad de la información basada en las buenas prácticas y conductas que adopten sus funcionarios para mitigar la materialización de escenarios que los puedan afectar negativamente.

2.2.1. ANTECEDENTES DEL PROBLEMA

Durante los últimos años el ataque informático con mayor afectación a nivel mundial fue el de WannaCry en mayo de 2017, el cual produjo una expansión de ransomware (*programa de software malicioso que infecta una computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.[4])* que afecto alrededor de 150 países, encontrando entre los más afectados países como: (Rusia, China, Ucrania, Taiwán, India y Brasil) y empresas impactadas como: el Servicio Nacional de Salud (NHS) del Reino Unido, Telefónica, FedEx, Hitachi y Renault.

Según información publicada por CISCO y Cybersecurity Ventures en su primera edición del Almanaque de Ciberseguridad del año 2019, mencionan: "Los hospitales son más vulnerables que cualquier otro tipo de organización en 2019. Los sistemas obsoletos, la falta de personal cibernético experimentado, datos muy valiosos y un incentivo adicional para pagar rescates a fin de recuperar los datos de los pacientes están magnetizando a los cibercriminales en el mercado de la salud y se prevé que los ataques de ransomware contra las organizaciones de atención médica se cuadrupliquen entre 2017 y 2020, y crecerán a 5 veces en 2021. Las prácticas de seguridad lamentablemente inadecuadas, las contraseñas débiles y compartidas, más las vulnerabilidades en el código, exponen a los hospitales a los perpetradores que intentan piratear tesoros de datos de pacientes."[5]

Los países Latinoamericanos que han reportado más casos de ataques informáticos durante los últimos años en el sector hospitalario son Brasil, México, Argentina, Chile y Colombia. Por ejemplo, el ataque informático del que fue víctima el Hospital San Juan de Dios en Armenia en abril del 2018 y en el cual se encripto información del servidor principal (información por la que ciberdelincuentes pedían pagar un rescate) como ocurre en todos los casos o en el caso de la Subred Sur de Salud de Bogotá sobre la cual se denunció un robo cibernético por valor de 1.500 millones de pesos el 6 de agosto de 2018[6].
Según informe publicado por la compañía Fortinet en el congreso Andicom 2019

[4] Kaspersky. Ransomware. {En línea}, {22 marzo de 2020}. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware
[5] MORGAN, Steve. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. {En línea}, {22 marzo de 2020}. Disponible en: https://cybersecurityventures.com/cybersecurity-almanac-2019/
[6] Caracol Radio. Investigan robo de 1500 millones de pesos de la salud en Bogotá. {En línea}, {22 marzo de 2020}. Disponible en: https://caracol.com.co/emisora/2018/08/21/bogota/1534872868_785885.html

realizado en Cartagena se demostró que durante el segundo trimestre del año: Colombia, fue uno de los países de la región LATAM con el nivel más alto de intentos de ataques informáticos, revelando una cifra que superaba los 41 billones y en donde los principales objetivos de los atacantes se concentraba en: las instituciones de gobierno y las empresas a nivel general.

El 100% de las denuncias realizadas por empresas y personas ante el CECIP (Centro Cibernético Policial), sitúan como principal incidente reportado durante el 2019 los casos de Phishing con un 42%, seguido de la suplantación de identidad con un 28%, él envió de malware con un 14% y los fraudes en medios de pago en línea con un 16%.

Considerando lo anterior, se afirma que los factores de ataques más comunes en Colombia son:

- Correos fraudulentos personalizados.
- El robo de identidad.
- Enmascaramiento de correo.
- Relación entre los dispositivos utilizados por las personas para realizar transacciones bancarias.
- El acceso desmedido a sistema informático.

Para Juan Carlos Puentes, Country Manager de Fortinet "*La ciberseguridad es un tema del cual tenemos que ocuparnos de manera prioritaria. Es necesario repensar la seguridad de forma integral para estar mejor preparados para prevenir, detectar y responder de manera automatizada a las amenazas*".[7]

2.2.2. PREGUNTA DE INVESTIGACIÓN

¿Cómo a través de la elaboración de un plan de concienciación en seguridad de la información se pueden prevenir posibles ataques informáticos que atenten contra la confidencialidad, integridad y disponibilidad de la información en las entidades de salud pública de Bogotá?

[7] Dinero. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. {En Línea}, {9 de mayo 2019}. Disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

2.2.3. VARIABLES DEL PROBLEMA

Dentro de las variables del problema que se plantean para el presente proyecto se mencionan:

- **Conciencia:** Hacer que alguien sea consciente de algo utilizando la introspección, el cual puede ser un proceso controlado que incluye medidas objetivas como tiempos de reacción y la asociación de palabras a través de las sensaciones y sentimientos de los individuos.

- **Integridad:** Garantizar que la información manejada por las entidades de salud no es alterada durante su proceso de almacenamiento o transporte.

- **Confidencialidad:** Garantizar que la información manejada por las entidades de salud es accedida únicamente por personal y/o entidades autorizadas.

- **Disponibilidad:** Asegurar que la información manejada por las entidades de salud están disponibles para uso y demanda de personal autorizado.

- **Sanción:** Decisión tomada por una entidad u organismo de control y que se le atribuye a una persona o entidad por el incumplimiento de una política, regla o norma que amerita un estricto cumplimiento.

III. JUSTIFICACIÓN

Gran parte de los problemas, riesgos y amenazas relacionados con el uso de la tecnología, las comunicaciones y los sistemas de información de las organizaciones a nivel general, se pueden mitigar dando cumplimiento a las políticas, procedimientos y las buenas prácticas que se tengan implementadas en su interior. Sin embargo, es sabido que las conductas inapropiadas de los empleados sobre el uso de estos medios para desempeñar sus tareas diarias, se han vuelto en uno de los mayores riesgos para el sector de la salud, el cual se encuentra sujeto actualmente a amenazas como: la exposición de datos personales de salud en la web a causa de ciberataques, el cierre de salas de urgencia producto de la propagación de ransomware, correos electrónicos falsos que afectan a socios, pacientes y personal clínico, etc.; convirtiéndolos así en uno de los blancos preferidos para que ciberdelincuentes puedan ejecutar sus ataques y saquen el mayor provecho afectando no solo las finanzas de este sector, sino también la confidencialidad e integridad de los pacientes.

Por tal motivo, el objetivo principal de este trabajo de grado es crear un plan de concienciación que pueda ser puesto en marcha en las entidades de salud del sector público de Bogotá con el que se logre contribuir a reducir las amenazas a las que se encuentran expuestos y fortalecer los temas que competen a las buenas prácticas que deben considerar sus funcionarios y contratistas, para garantizar no solo la confidencialidad, integridad y disponibilidad de la información que manejan, sino también su reputación y buen nombre.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Elaborar un plan de concienciación dirigido a los funcionarios de las entidades de salud del sector público de Bogotá, con el que se genere un cambio conductual respecto a la importancia de la seguridad de la información.

3.2. OBJETIVOS ESPECÍFICOS

- Identificar las necesidades de concienciación de los funcionarios de la entidades de salud pública de Bogotá, las cuales alimentaran el diseño del plan que se busca elaborar.

- Revisar las políticas, procesos y procedimientos implementados en las entidades de salud del sector público de Bogotá para diseñar el plan de concienciación.

4. MARCOS DE REFERENCIA

4.1. MARCO CONCEPTUAL

Para poder entrar en contexto, el autor considera necesario que el lector se familiarice con algunos conceptos importantes, los cuales le ayudaran a comprender el panorama sobre el cual se está trabajando y que se adhieren a los conceptos definidos bajo la norma Técnica Colombiana ISO 27000.(2017):[8]

Seguridad de la Información: preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. Esta debe garantizar que solo las personas autorizadas tienen acceso a la información necesaria de acuerdo con su roles y responsabilidades dentro de una organización.

Integridad: Propiedad de salvaguardar la exactitud y la integridad. Entiéndase como integridad de la información a la precisión de los datos que se transportan de un punto A a un punto B, sin que los mismos sufran modificaciones, alteraciones o algún cambio que comprometa la veracidad de dicha información, lo cual por mínimo que parezca, podría acarrear consecuencias desfavorables para una organización.

Disponibilidad: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada. "Se entiende por disponibilidad al grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. La disponibilidad significa que el sistema, tanto en su parte hardware como software, se mantiene funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo.[9]"

---

[8] ISO/IEC 27000. (2017). Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y vocabulario.

[9] SÁNCHEZ GARRETA, José salvador, *et al*. [Online]. Ingeniería de proyectos informáticos: Actividades y procedimientos. Castellón de la Plana: Publicacions de la Universitat Jaume I. 2003.p. 103. Disponible en: https://books.google.com.co/books?id=MXTI43ThoS4C&printsec=frontcover&dq=inauthor:%22Jos

Diferencia entre seguridad de la información y seguridad informática: a pesar de que estos conceptos están relacionados al tener como objetivo salvaguardar los pilares de la información; su diferencia radica en que la *Seguridad de la Información* hace parte de la estrategia de una organización y abarca todas las medidas, políticas, procesos y procedimientos destinados para proteger los datos de valor incluyendo así mismo a sus colaboradores quienes son parte fundamental para el desarrollo de un adecuado SGSI (Sistema de Gestión de Seguridad de la Información), mientras que la *Seguridad Informática* es el conjunto de herramientas disponibles y utilizadas como: (Redes, software, hardware, infraestructura en general, etc.) para proteger la información y los datos que se encuentran alojados en los sistemas de una organización.

Dato personal: información que pueda llegar a vincular o asociar a un individuo o individuos con el entorno que los rodea.

Es considerado como un dato personal: Nombre(s), apellidos, fecha de nacimiento, número de identificación ciudadana, dirección física, dirección de correo electrónico, número telefónico, estado civil, datos de salud, lugar de trabajo, redes sociales, localización; etc.

Datos sensibles[10]: se entienden por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenecía a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y a los datos biométricos.

Historia Clínica[11]: es el registro obligatorio de las condiciones de salud del paciente. Es un documento privado sometido a reserva, que únicamente puede ser conocido por terceros, previa autorización del paciente o en casos previstos por la ley.

[10] Ibíd., p 4.
[11] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 23 (28, febrero,1981). Por la cual se dictan normas en materia de Ética Médica. Bogotá, 1981. 14 p.

Tratamiento[12]: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

¿De qué nos protegemos?

El estar haciendo uso de las tecnologías de la información de las cuales disponemos actualmente, hace que los datos que son almacenados y manipulados se expongan ante tres factores que se deben considerar y tener en cuenta para evitar la materialización de posibles ataques informáticos.

Amenaza: Se pueden considerar como amenaza el entorno en que nos encontramos el cual incluye agentes externos como: la internet, la competencia, las compañías proveedoras de servicios, etc. e internos como: las propias personas, malas decisiones, equipamiento defectuoso y que se encuentre en servicio; y en casos extremos, desastres naturales que se puedan presentar y puedan causar un incidente o daño no deseado a un sistema o entidad.

Riesgo: Es la probabilidad de que una amenaza se materialice aprovechándose de una debilidad existente sobre un activo (s) de una organización y la cual pueda ocasionarle daños o pérdidas.

Vulnerabilidad: Son características**,** debilidades o fallas identificadas sobre un activo o sistema de información de una organización que de ser aprovechados por un atacante, podría exponer la confidencialidad, integridad y disponibilidad de su información.

[12] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (17,octubre,2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá, 2012. p 2.

4.2. MARCO TEÓRICO

En el momento de garantizar la seguridad de una organización sin importar su naturaleza además de contar con las medidas técnicas y legales correspondientes, es de suma importancia incluir el factor humano, considerando que los más grandes errores de seguridad informática resultan en torno a los descuidos que se presentan en el desarrollo de actividades diarias desarrolladas por las personas.

Es claro que las entidades del sector salud por lo general no emplean colaboradores con habilidades destacadas o avanzadas en tecnologías de la información o con formación precisa en materia de seguridad para el cumplimiento de las labores que se deben desempeñar - salvo el personal del área de tecnología, y sin intención olvidan el gran número de amenazas internas a las que se encuentran expuestos a la hora de planificar la estrategia de seguridad. Esta situación se agrava en entornos abiertos a Internet, donde no es un secreto para nadie el crecimiento abrumador de la tecnología acompañado paralelamente al aumento de las amenazas que se van presentando.

Con el fin de proteger la información, las organizaciones -incluyendo el sector salud- han optado por la adopción e implementación de lineamientos a la vanguardia que los apoyen a cumplir con su estrategia de negocio garantizando siempre la seguridad de su información. Estos lineamientos son estudiados de acuerdo a la necesidad y tamaño del negocio, siendo posteriormente incluidos en un documento denominado: Política de Seguridad de la Información, el cual requiere de una previa revisión, aprobación, socialización y cumplimiento por parte de las partes interesadas para el cual fue diseñado: empleados, proveedores y terceros.

Para que lo estipulado en la política de seguridad de la información se cumpla de manera satisfactoria por parte de su público objetivo, se hace necesario no solo de la socialización de su contenido, sino también del uso de estrategias de sensibilización y concienciación prácticas que de manera sencilla pero eficaz logren captar la atención del público hacia el cual fue diseñada y sirvan para garantizar su optimo cumplimiento.

De acuerdo con cifras relatadas por el National Security Institute, en promedio, alrededor del 80% de la inseguridad de la información ocurre por fallas de seguridad al interior de la organización, representado por todas aquellas personas que de una u otra manera y sin ser consientes incumplen con requisitos mínimos que violan o atentan contra la confidencialidad, integridad y disponibilidad de la información. Uno de los tantos ejemplo que se podría mencionar sería el caso del usuario distraído que escribe su contraseña a la vista de quien lo está rodeando, o el que se lleva información sensible para su hogar sin una debida autorización o simplemente, el empleado que permite que los visitantes husmeen por su área de trabajo sin acompañamiento alguno.

Por lo anterior, es de gran importancia que las organizaciones independientemente del sector al que pertenezcan, cuenten no solo con mecanismos de infraestructura tecnológica que las protejan de las miles de amenazas a las que se encuentran expuestas, sino también que puedan contar con personal en condiciones de actuar de manera apropiada y consiente en caso de presentarse escenarios de riesgo que las puedan afectar reputacional, económica y legalmente a causa de individuos malintencionados.

Cultura organizacional en seguridad de la información.

Cuando se habla de cultura organizacional, se hace referencia a todo un conjunto de hábitos, experiencias, costumbres y valores que adquiere un grupo de personas que integran una compañía y que genera una identidad que fortalece o debilita los objetivos planteados para el futuro éxito de sus metas trazadas. En efecto, se entiende que mientras exista mayor pertenencia y adhesión de estos comportamientos por parte de los funcionarios ante los valores y principios propuestos, mayor y mejores resultados se obtendrán como beneficio para la organización. No obstante, cabe resaltar que si ocurre todo lo contrario los resultados no serán los esperados y lo que se obtendrá es la apariencia de una organización desintegrada.

Por lo tanto, si se quiere trabajar en la gestión de un cultura basada en los estándares de la seguridad de la información, se debe comenzar por diseñar, desarrollar e implementar las medidas necesarias para que todos y cada uno de los funcionarios que hacen parte de la organización se transformen en sus mejores aliados a la hora de dar cumplimiento a los objetivos organizacionales planteados.

Para que todo esto converja, será necesaria la buena gestión que desempeñe el

grupo de TI designado para socializar y crear dicha cultura de seguridad de la información a través de planes de concienciación y sensibilización en donde se resalte en primer lugar la importancia que tiene cada uno de los funcionarios dentro de la organización de acuerdo con sus responsabilidades para con la misma. De este modo la cultura que se genere estará basada en principios de integración, orientación hacia los lineamientos estratégicos, en la visión, trabajo en equipo y en una adecuada adaptación en donde prime la comunicación asertiva, la motivación y una alta pertenencia por proteger los objetivos de la organización para quien prestan sus servicios.

Consideraciones a tener en cuenta para la creación de un plan de concienciación y sensibilización en seguridad de la información.

Cuando una organización implementa un SGSI (Sistema de Gestión de Seguridad de la Información), debe cerciorase que para su efectivo cumplimiento, hay que hacer partícipe a sus colaboradores quienes deberán alinearse para trabajar acorde a las políticas, procesos y procedimientos establecidos. Para que esto suceda, primero se debe tener la certeza de que los funcionarios se encuentran preparados y son conscientes de la responsabilidad que conlleva el lograr mantener un sistema de este tipo.

Por lo anterior se hará necesario crear un plan de concienciación sobre seguridad de la información el cual deberá considerar los siguientes aspectos para su adecuado diseño, desarrollo, implementación, seguimiento y mejora continua:

- Identificar y estudiar las necesidades de concienciación de todos los funcionarios de la organización (desde empleados, supervisores, gerentes funcionales, hasta los gerentes de nivel ejecutivo).
- Selección del modelo adecuado para el desarrollo del plan.
- Desarrollar y definir la temática que será incluida y contemplada en el plan de concienciación.
- Planificar un calendario para su respectivo despliegue y socialización.
- Preparación del material, el cual siempre debe responder y alinearse a las necesidades estratégicas del negocio.

Algunos de los aspectos que se aconsejan tratar en estos plan de concienciación incluyen:

- Uso de contraseñas.
- Protección contra virus.
- Cumplimiento de la política de seguridad.
- Instrucciones para el adecuado uso del correo electrónico.
- Adecuado uso de Internet.
- Backups.
- Manejo y reporte de incidentes.
- Ingeniería Social.
- Uso de software permitido y no permitido.
- Manejo adecuado de medios removibles (USB, discos duros, dispositivos móviles, etc.).

Según reporte de la *Healthcare Information and Management Systems Society (HIMSS)* sobre la ciberseguridad en el sector sanitario en los Estados Unidos de América, demostró la integración de prácticas de seguridad como formas de defensa considerando el sofisticado pero peligroso escenario digital al que se expone y los frecuentes reportes de brechas de seguridad en hospitales y clínicas a nivel global.

Dentro de las recomendaciones que aborda dicho reporte se puede observar un alto interés por que las compañías del sector salud a nivel mundial cuenten con al menos los siguientes requisitos:

- Contar con un Director en seguridad de la información – CISO – que cuente con los conocimientos y en nuevas tecnologías y una amplia experiencia respecto a seguridad de la información.

- Desarrollar programas de evaluación de riesgo, en donde se incluyan no solo factores externos, sino que también se contemple el riesgo del “atacante interno” con el cual se pueda atender y disminuir los ataques o acciones no intencionales que puedan afectar la información que se maneja de los pacientes.

- Implementar planes de concientización que involucre a todo el personal médico, operativo y administrativo de la institución de salud.

- Desarrollar pruebas de vulnerabilidades sobre la infraestructura que soporta los sistemas de información y la gestión administrativa de la institución de salud, teniendo en cuenta los dispositivos médicos disponibles con los proveedores respectivos.

- Incorporar y aplicar marcos de gestión de tecnología de información y seguridad de la información generales (como los ISO, las guías del NIST y COBIT), así como aquellos específicos de la industria como HITRUST o la HIPAA - Health Insurance Portability and Accountability Act de 1996.

4.3. MARCO JURÍDICO

De acuerdo con las disposiciones legales en Colombia y a las leyes y/o regulaciones que se contemplan para proteger la seguridad de la información en las entidades de salud del sector público, a continuación se listan algunas de las más importantes:

Ley 23 de 1981 Art.34: por la cual se dictan normas en materia de ética médica y se informa que la Historia Clínica es el registro obligatorio de las condiciones de salud del paciente. Es documento privado, sometido a reserva, que únicamente puede ser conocido por terceros, previa autorización del paciente o en los casos previstos por la ley.

Ley 594 de 2000: Ley general de archivos – Criterios de Seguridad.

Ley 1266 de 2008: Habeas Data Financiera y seguridad en Datos Personales.

Ley 594 de 2000 y todos los acuerdos promulgados por el Archivo General de la Nación.

Ley 1273 de 2009: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado *"de la protección de la información y de los datos"*- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1581 de 2012: por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014: Ley de Transparencia y Acceso a la Información Publica Nacional.

Ley 2015 de 2020: por medio del cual se crea la Historia Clínica Electrónica Interoperable y se dictan otras disposiciones.

Resolución 839 de 2017: por la cual se establece el manejo, custodia, tiempo de retención, conservación y disposición final de los expedientes de las historias clínicas, y la reglamentación del procedimiento que deben adelantar las entidades del SGSSS (*Sistema de Seguridad Social en Salud*)-, para el manejo de estas en caso de liquidación.

Resolución 1995 de 1999: por la cual se establecen normas para el manejo de las Historias Clínicas.

4.4. ESTADO DEL ARTE

La protección de los datos personales surgió ligada al derecho a la intimidad, reconocido en varios instrumentos del derecho internacional de los derechos humanos.

Hechos sucedidos como el uso de la información del censo y sus respectivos documentos se utilizaron durante la segunda guerra mundial en Alemania para ubicar a las familias judías y de más población víctimas del genocidio, generaron que una vez concluida la guerra, se apelara por el derecho a la intimidad en donde prevaleciera la protección de dicha información a nivel regional y nacional.

A nivel internacional, en 1948 se reconoció por primera vez el derecho a la intimidad y el cual se plasmó en el artículo 12 de la Declaración de los Derechos Humanos en donde se dispuso que: toda persona debe ser protegida contra injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataque contra su honra y reputación.

En el caso de Colombia y teniendo en cuenta que desde hacía años atrás existía cierta preocupación por la protección de los datos personales, se creó la Ley 23 de 1981 "*por la cual se dictan normas en materia de ética médica",* y cuyo artículo 34 dispone que la historia clínica "*es un documento privado sometido a reserva que únicamente puede ser reconocido por terceros previa autorización del paciente o en los casos previstos por la ley"*, y no fue sino hasta el año 1991 que se reconoció el

derecho al habeas data por primera vez en su constitución política.

Panorama de amenazas informáticas en el sector salud.

Contemplando el acelerado crecimiento tecnológico y las amenazas asociadas, se ha evidenciado la necesidad de adaptación e incorporación de nuevas tecnologías por parte de las empresas del sector salud, las cuales han dejado en segundo plano las practicas adecuadas para una correcta gestión de los sistemas de información adquiridos; convirtiéndose así, en un escenario clave para los ciberdelincuentes que ya no solo se interesan por la manipulación abusiva de los dispositivos médicos, sino que ahora están apuntando sus ataques sobre las interfaces que se han venido integrando en el ejercicio de sistematización con el fin de afectar la integridad y disponibilidad de los pacientes mediante el robo de la información que aquí se almacena. Como es de esperarse y como pasa en otros sectores de la industria, los sistemas de administración de salud deben entender que cualquier incorporación de tecnología para el manejo de información en su negocio, debe dar respuesta afectiva y oportuna a la manera en que se va a brindar atención, en este caso: a los pacientes.

Amenazas tan frecuentes como lo son: el acceso no autorizado a la infraestructura, la suplantación de identidad, la fuga de información, la pérdida de datos, la denegación de servicios, la modificación no autorizada de datos, el secuestro de datos, el malware elaborado a la medida y los atacantes internos, hacen del sector salud, un punto objetivo para que los ciberdelincuentes logren llevar a cabo de manera satisfactoria sus actos delincuenciales, teniendo en cuenta que la concientización de la protección de la información en el personal médico es baja, y la mayor responsabilidad se encuentra delegada en los profesionales de TI que los apoyan desde la infraestructura tecnológica

Si esta situación no se trata desde la adopción de la toma de conciencia por parte los funcionarios a nivel general (incluidos los médicos y demás profesionales de la salud) y el establecimiento de una cultura organizacional que integre lineamientos, políticas, procesos y procedimientos que garanticen la seguridad de la información que maneja la entidad, las empresas del sector salud se estarán viendo expuestas a la pérdida de credibilidad y a un alto grado de desconfianza por parte de los pacientes respecto a la exigencia del cuidado que ameritan de su información.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, en Colombia, la estrategia de Gobierno en Línea (GEL), liderada por el Ministerio TIC, diseño el modelo de seguridad y privacidad de la información, documento guía para empresas del sector público y privado que les permite mejorar los estándares de seguridad de la información, de acuerdo con las nuevas tendencias tecnológicas y sus debidas actualizaciones con el fin de estar siempre alineados con mejores prácticas, normas, marcos de referencia y recomendaciones hechas por organizaciones como el Convenio de Budapest y la Organización para la Cooperación y el Desarrollo Económico (OCDE), Organización de Estados Americanos - OEA, entre otros; donde las entidades del estado se vean beneficiadas con la construcción e implementación del mismo.

Ahora bien, cabe resaltar la adopción de Historia Clínica Electrónica Interoperable a través de la ley 2015 de 2020; considerándose como uno de los grandes desafíos que se vienen para el país al querer garantizar la interoperabilidad de todo el sistema de salud con el objetivo de que cada uno de los componentes que la conforman pueda tener una comunicación efectiva y ejecuten con agilidad y eficiencia las actividades relacionadas, panorama que igualmente abre las puertas a un nuevo marco de sumo cuidado en cuanto a la adopción y cumplimiento de estándares técnicos internacionales en materia de salud, como el Health Level Seven (HL7), el Health Insurance Portability and Accountability Act (Ley HIPPA), o las normas de la Unión Europea para la información en salud y las comunicaciones CEN/TC215.

5. METODOLOGÍA

5.1. FASES DEL TRABAJO DE GRADO

En cumplimiento de la política y el plan de seguridad de la información definidos en las entidades de salud del sector público de Bogotá que tienen como objetivo preservar la confidencialidad, integridad y disponibilidad de los activos con los que cuentan; para el desarrollo de este proyecto se tuvo en cuenta las fases que según el Plan de capacitación, sensibilización y comunicación de la seguridad de la información generado por el MINTIC y la publicación especial de la NIST SP 800-50 (*Creación de un programa de capacitación y concientización sobre seguridad de TI*) se deben considerar para diseñar un plan de concienciación efectivo. Dentro de estas fases se destacan aspectos importantes como:

- Identificar las actividades a ser desarrolladas para cumplir con las metas de entrenamiento de la organización.
- Enfocarse en el alcance, fuentes de información actualizada y disponible, y contenido del material de entrenamiento.
- Direccionar de manera adecuada la forma en que será comunicado el material diseñado.
- Indicar como mantener el plan actualizado, monitorizando su efectividad,

Por lo anterior, para la definición y elaboración de este plan se definieron 3 fases, las cuales se describen a continuación.

Figura 1 Fases para el desarrollo del proyecto.

- **Fase de Diagnóstico:** En esta fase se identificaron las necesidades de concienciación de funcionarios de las entidades de salud del sector público de Bogotá, a través del diligenciamiento de encuestas.

- **Fase de Análisis:** Concluida la fase de diagnóstico y de acuerdo con los resultados obtenidos, se procedió a seleccionar los temas sobre los cuales se requiere reforzar el conocimiento y la conducta de los funcionarios de las entidades de salud del sector público de Bogotá.

- **Fase de Desarrollo:** Una vez identificados los temas sobre los que se encontraron mayores falencias, se procedió a seleccionar la temática que se considera más importante y que se incluyeron en el plan de concienciación.

5.2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Los instrumentos utilizados para realizar el diagnostico e identificar los temas sobre los que se hace necesario implementar el plan de concienciación en las entidades de salud del sector público de Bogotá fueron dos:

El primer instrumento consistió en el diligenciamiento de La Herramienta de Autodiagnóstico de INCIBE (Instituto Nacional de Ciberseguridad - España) disponible en su página web: (https://adl.incibe.es/), la cual es una encuesta que consta de 35 preguntas abiertas, y que tiene como objetivo evaluar la seguridad de un negocio en función de cómo se está utilizando la tecnología. Esta herramienta fue diligenciada por 3 referentes de algunas de las entidades de salud del sector público de Bogotá y quienes por temas de confidencialidad se abstienen de mencionar sus nombres o cargo dentro de la entidad. **Ver Anexo 1.**

El segundo instrumento consistió en la creación y posterior diligenciamiento de una encuesta de 21 preguntas (abiertas y cerradas) formuladas a través de la herramienta de google drive por el autor del proyecto y la cual fue aplicada a funcionarios de algunas de las entidades de salud del sector público de Bogotá, quienes por temas de confidencialidad se abstienen de mencionar sus nombres o cargo dentro de la entidad. **Ver Anexo 2.**

5.3. POBLACIÓN Y MUESTRA

Para el desarrollo de este proyecto se contó con la colaboración de tres (3) funcionarios con cargos relevantes dentro de algunas de las entidades de salud pública de Bogotá, así como también con la ayuda de cincuenta y ocho (58) funcionarios con cargos operacionales de diferentes entidades de este mismo sector y quienes por temas de confidencialidad se abstuvieron de mencionar sus nombres o cargos dentro de las entidades para las cuales prestan sus servicios.

5.4. ALCANCES Y LIMITACIONES

Alcances

El alcance de este proyecto es diseñar un plan de concienciación que sirva como modelo y que incluya los principales temas sobre los cuales se debe concienciar a los funcionarios de las entidades de salud del sector público de Bogotá para mitigar la materialización de los riesgos asociados y que afectan la confidencialidad, integridad y disponibilidad de la información que aquí se maneja.

Limitaciones

Dentro de las limitaciones definidas, cabe mencionar que solo se hará el diseño y la elaboración del modelo de un plan de concienciación dirigido a las entidades de salud del sector público de Bogotá. El mismo no se replicará ni se pondrá a prueba sobre los funcionarios de las entidades que participaron, teniendo en cuenta el compromiso de confidencialidad adquirido.

6. PRODUCTOS A ENTREGAR

Los productos a entregar una vez finalizado el proyecto son:

1. Plan de concienciación sobre la importancia de la seguridad de la información en las entidades de salud del sector público de Bogotá. **Ver Anexo 3.**
2. Infografía sobre Plan de Concienciación propuesto.
3. Articulo IEEE.

7. ENTREGA DE RESULTADOS E IMPACTOS

7.1. PLAN DE CONCIENCIACIÓN

Diagnostico.

Para la elaboración del plan de concienciación, previamente se revisaron las políticas de seguridad de la información definidas en las entidades de salud del sector público de Bogotá, identificándose que para las 4 subredes de salud que la conforman, el objetivo principal está basado en garantizar la triada de la información de los activos con los que cuentan y con los que buscan brindar un servicio consolidado, sostenible, confiable, y de calidad.

Validados los documentos relacionados con seguridad de la información y los cuales se encuentran publicados en los sitios web correspondientes de cada una de las subredes de salud, se pudo identificar que no existen registros de seguimiento recientes que garanticen que las entidades están trabajando en pro del cumplimiento de sus políticas de seguridad de la información.

Para corroborar lo anterior, se solicitó el diligenciamiento de las siguientes herramientas propuestas, a un grupo de funcionarios miembros del sector, previamente seleccionados:

- Herramienta Autodiagnóstico – INCIBE.
- Encuesta: Seguridad de la Información en su entorno de trabajo.

Una vez diligenciadas, se procedió a analizar y comparar los resultados obtenidos para identificar y seleccionar los temas sobre los cuales se hace necesario reforzar las buenas prácticas de comportamiento de los funcionarios que contribuyan a garantizar la seguridad de la información en su organización y así mismo mitigar los riesgos a los cuales se encuentran actualmente expuestos.

Análisis de resultados.

A. Herramienta Autodiagnóstico – INCIBE.

Una vez obtenidos los resultados arrojados por la herramienta de Autodiagnóstico – INCIBE (Ver Anexo 1), los mismos fueron tabulados y posteriormente promediados para valorar la percepción que tienen los 3 funcionarios encuestados frente a la seguridad de la información sobre las entidades de salud del sector público en las que prestan sus servicios profesionales considerando los criterios evaluados por la herramienta.

RESULTADOS REFERENTE 1

CRITERIO EVALUADO	NIVEL DE RIESGO CALCULADO POR LA HERRAMIENTA	PORCENTAJE CALCULADO POR LA HERRAMIENTA
PERSONAS	MEDIO	54,50%
PROCESOS	MEDIO	41,70%
TECNOLOGÍA	MEDIO	44,80%
TOTAL		**47,00%**

RESULTADOS REFERENTE 2

CRITERIO EVALUADO	NIVEL DE RIESGO CALCULADO POR LA HERRAMIENTA	PORCENTAJE CALCULADO POR LA HERRAMIENTA
PERSONAS	ALTO	72,00%
PROCESOS	MEDIO	65,00%
TECNOLOGÍA	ALTO	75,00%
TOTAL		**70,67%**

RESULTADOS REFERENTE 3

CRITERIO EVALUADO	NIVEL DE RIESGO CALCULADO POR LA HERRAMIENTA	PORCENTAJE CALCULADO POR LA HERRAMIENTA
PERSONAS	ALTO	10%
PROCESOS	MEDIO	50%
TECNOLOGÍA	ALTO	0%
TOTAL		**20%**

Tabla 1 Resultados herramienta Autodiagnóstico - INCIBE.

Para calcular este promedio, a cada uno de los niveles de riesgo definidos por la herramienta de autodiagnostico se le asigno un valor (usando una escala de 1 a 3) como se puede apreciar en la Tabla 2 y posteriormente se generó la Tabla 3, sobre la cual se obtuvo el resultado promedio esperado:

NIVEL DEL RIESGO	VALOR ASIGNADO
BAJO	1
MEDIO	2
ALTO	3

Tabla 2 Valores de Riesgo Herramienta Autodiagnóstico INCIBE

REFERENTE / CRITERIO EVALUADO	REFERENTE 1	REFERENTE 2	REFERENTE 3	PROMEDIO GENERAL
PERSONAS	2	3	1	2
PROCESOS	2	2	2	2
TECNOLOGÍA	2	3	3	2,7

Tabla 3 Promedio general de resultados Herramienta de Autodiagnóstico INCIBE

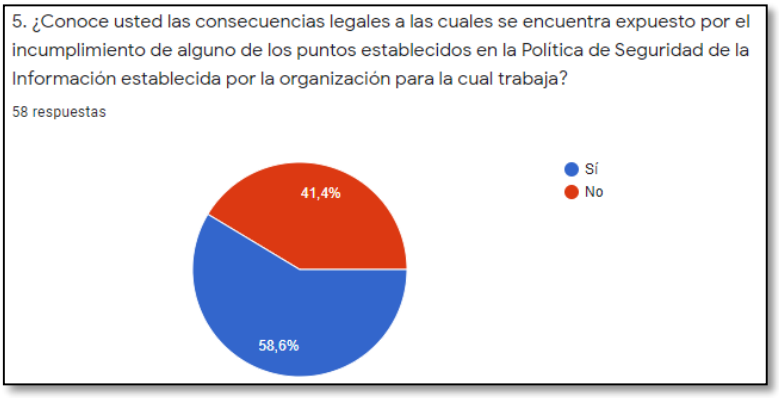
El resultado arrojado en la Tabla 3 concluye que según la percepción de los referentes encuestados, el nivel de riesgo sobre el cual se debe prestar mayor atención actualmente en las entidades de salud del sector público de Bogotá se encuentra enfocado en primer lugar a aspectos de Tecnología, el cual dio un valor de riesgo alto, demostrando así la existencia de una gran brecha de seguridad que podría ser aprovechada por los delincuentes informáticos.

También se puede observar que para los criterios de: (personas y procesos) el resultado arrojo un nivel de riesgo: Medio, presumiéndose igualmente la falta de cultura en seguridad de la información sobre un eslabón tan importante como lo son los funcionarios y quienes de no contar con los hábitos y comportamientos adecuados podrían estar ayudando en cierta forma, a que los ciberdelincuentes logren penetrar más fácilmente la tecnología actualmente en uso, convirtiéndolos en un blanco objetivo muy fácil de vulnerar y afectar.

B. Encuesta: Seguridad de la Información en su entorno de trabajo.

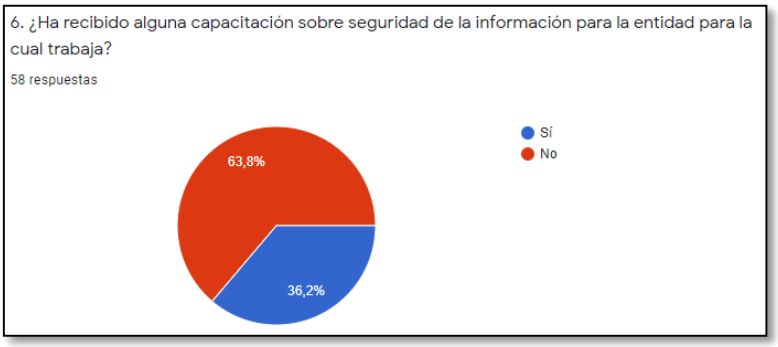
Los resultados arrojados por la encuesta practicada a los 58 funcionarios, demostraron lo siguiente:

- Un 41,4% de los funcionarios encuestados manifestaron desconocimiento en cuanto a las consecuencias legales a las que se encuentran expuestos por el incumplimiento a la Política de Seguridad de la Información establecida por la entidad.



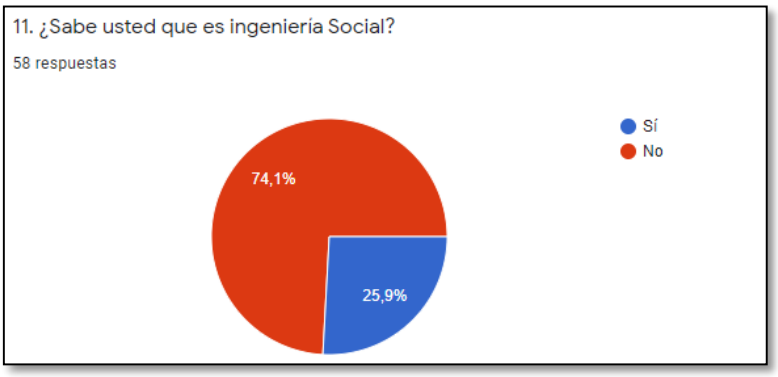
Gráfica 1 Pregunta 5. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

- Un 63,8% de los funcionarios encuestados manifestaron la falta de capacitación sobre Seguridad de la Información por parte de la organización para la cual trabajan.



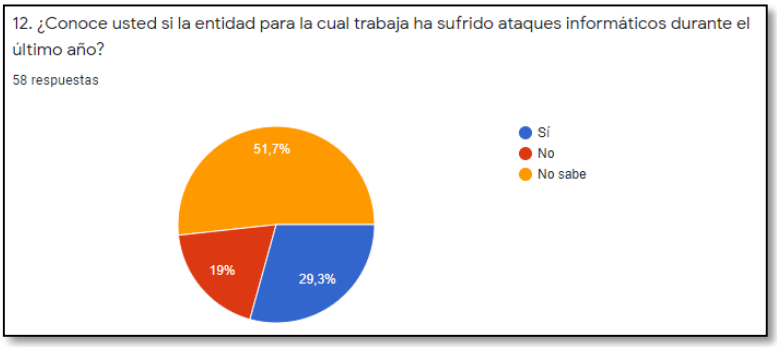
Gráfica 2 Pregunta 6. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

- Un 74,1% de los funcionarios encuestados manifestaron desconocimiento respecto a lo que es la Ingeniería Social.



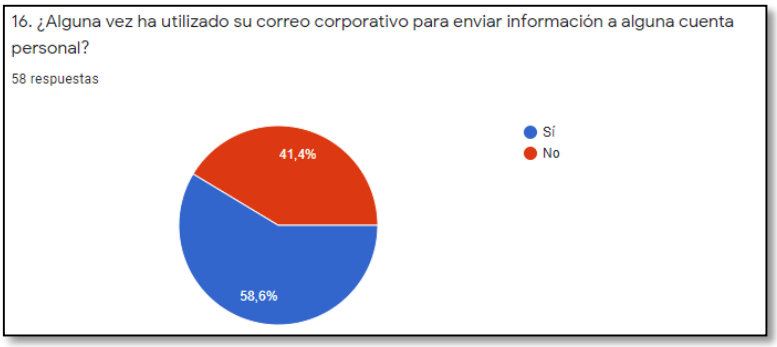
Gráfica 3 Pregunta 11. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

- Un 51,7% de los funcionarios encuestados manifestaron no saber si la entidad para la cual trabajan ha sufrido ataques informáticos durante el último año.



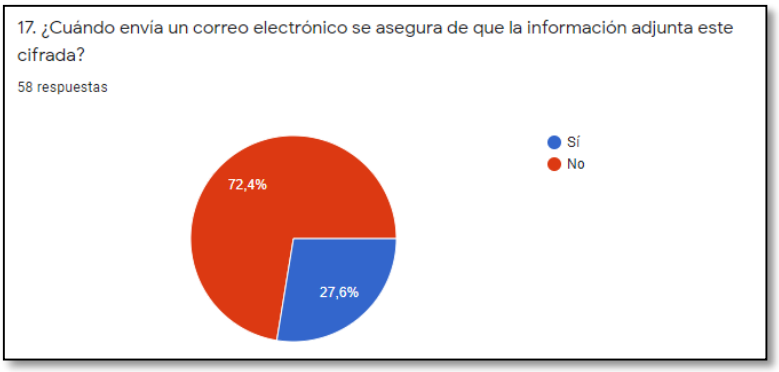
Gráfica 4 Pregunta 12. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

- Un 58,6% de los funcionarios encuestados manifestaron haber utilizado su cuenta de correo electrónico corporativo para enviar información a cuentas de correo electrónico personal.



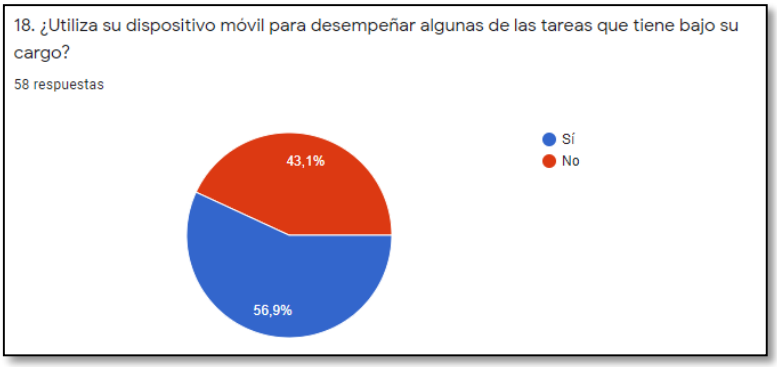
Gráfica 5 Pregunta 16. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

- Un 72,4% de los funcionarios encuestados manifestaron que al enviar correos electrónicos no cifran la información adjunta.



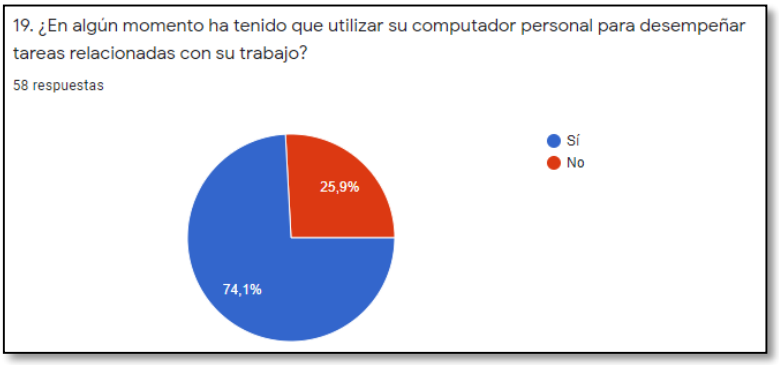
Gráfica 6 Pregunta 17. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

- Un 56,9% de los funcionarios encuestados manifestaron haber utilizado su dispositivo móvil para desempeñar algunas de las tareas que tienen bajo su cargo.



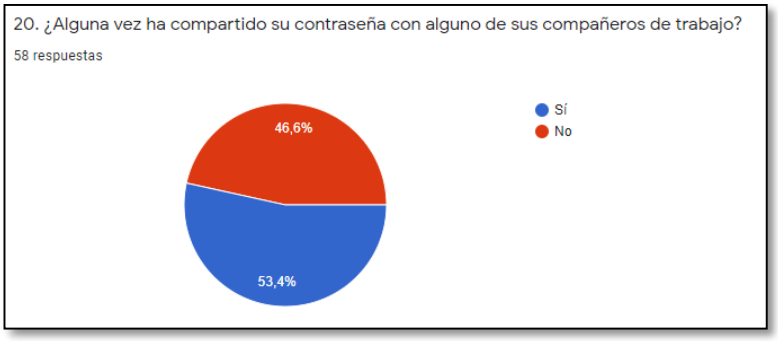
Gráfica 7 Pregunta 18. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

- Un 74,1% de los funcionarios encuestados manifestaron haber utilizado su computador personal para desempeñar tareas relacionadas con su trabajo.



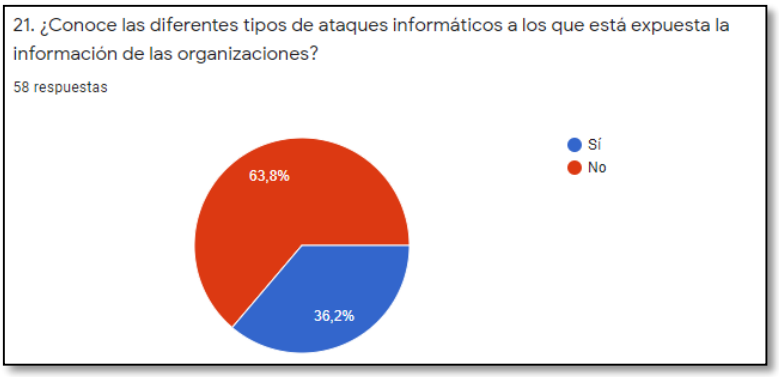
Gráfica 8 Pregunta 19. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

- Un 53,4% de los funcionarios encuestados manifestaron haber compartido su contraseña con alguno de sus compañeros de trabajo.



Gráfica 9 Pregunta 20. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

- Un 63,8% de los funcionarios encuestados manifestaron desconocer los diferentes tipos de ataques informáticos a las que se encuentra expuesta la información dentro de las organizaciones para las cuales trabajan.



Gráfica 10 Pregunta 21. Encuesta Seguridad de la Información Entidades de Salud del Sector Público.

Desarrollo

Comparando los resultados obtenidos una vez aplicadas las dos herramientas seleccionadas, se pudo corroborar que actualmente los funcionarios que laboran en las entidades de salud del sector público de Bogotá carecen de una cultura basada en las buenas prácticas con la que se garantice la seguridad de la información y con la cual se fortalezca el uso de la tecnología que según el resultado arrojado por la herramienta de Autodiagnóstico - INCIBE, representa un riesgo alto para este sector.

En consecuencia, se logra identificar que los temas sobre los que se debe abordar el plan de concienciación para las entidades de salud del sector público de Bogotá, debe incluir dentro de sus temas a reforzar:

1. Socialización de la Política de Seguridad de la Información de la entidad de salud y las consecuencias derivadas por su incumplimiento.
2. Capacitación sobre Seguridad de la Información.
3. Reconocimiento sobre que es la Ingeniería Social.
4. Uso adecuado de contraseñas.
5. Uso seguro del correo electrónico.
6. Seguridad sobre dispositivos móviles.
7. Reconocimiento de los diferentes ataques informáticos.

A través del refuerzo de los aspectos anteriormente identificados, el sector evaluado se verá beneficiado al lograr que sus funcionarios cuenten con los conocimientos mínimos y las actitudes pertinentes para hacer un mejor uso de los medios dispuestos para desempeñar sus labores diarias, respetando y cumpliendo así las políticas establecidas por la entidad de salud, identificando de manera más fácil los riesgos a los que se encuentran expuestos; logrando mitigar la materialización de ataques que se puedan materializar por su mal uso .

Como producto de apoyo a este análisis, se elabora un plan de concienciación (Ver Anexo 3) basado en las buenas prácticas y recomendaciones propuestas en el Plan de capacitación, sensibilización y comunicación de la seguridad de la información generado por el MINTIC y en la publicación especial NIST SP 800-50, el cual consta de:

- Introducción.
- Antecedentes generales.
- Objetivo.
- Alcance
- Usuarios y necesidades.
- Estrategia de aplicación del plan de concienciación.
- Temas clave a concienciar.
- Referencias.

7.2. INFOGRAFIA

Como estrategia para promocionar el plan de concienciación producto del trabajo realizado y lograr su aceptación por parte del sector seleccionado, se diseñó la siguiente infografía que comprende de manera muy visual y fácil de entender, los pasos a tener en cuenta para poder implementar un plan de concienciación efectivo en seguridad de la información en cualquier entidad de salud del sector público de Bogotá.

Imagen 1 Plan conciencia – Seguridad de la Información: Sector Salud. Fuente: El autor.

8. NUEVAS ÁREAS DE ESTUDIO

Se propone que el modelo del plan de concienciación propuesto sea enfocado a garantizar la seguridad de la información de las historias clínicas de los pacientes, siendo esta información muy importante y también vulnerable para las entidades de salud a nivel general y más aún, considerando el proyecto de ley 2015 aprobado el 31 de enero de 2020 y con el que se busca crear la Historia Clínica Electrónica Interoperable en Colombia.

9. CONCLUSIONES

De acuerdo con los resultados obtenidos una vez aplicadas las herramientas de diagnóstico, se pudo identificar que actualmente los funcionarios de las entidades de salud del sector público de Bogotá, carecen de conciencia respecto a las buenas prácticas que deben mantener para dar cumplimiento a la política de seguridad de la información y con las cuales se pueda mitigar la materialización de las amenazas a las cuales se encuentra expuesto el sector.

De acuerdo con los resultados obtenidos una vez aplicadas las herramientas de diagnóstico, se logró identificar que los temas sobre los que inicialmente se debe abordar el plan de concienciación para las entidades de salud del sector público de Bogotá, debe incluir: La socialización de la Política de Seguridad de la Información de la entidad de salud y las consecuencias derivadas por su incumplimiento, capacitación sobre seguridad de la información, reconocimiento sobre que es la Ingeniería Social, el uso adecuado de contraseñas, el uso seguro del correo electrónico, seguridad sobre dispositivos móviles y reconocimiento de los diferentes ataques informáticos.

Con la implementación del plan de concienciación propuesto, las entidades de salud del sector público de Bogotá se verán beneficiadas; ya que lograrán que sus funcionarios cuenten con los conocimientos mínimos y las actitudes propias para hacer un mejor uso de los medios dispuestos para desempeñar sus labores diarias, respetando y cumpliendo así las políticas establecidas por la entidad de salud, identificando de manera más efectiva los riesgos a los que se encuentran expuestos y obteniendo como resultado la reducción de ataques que se puedan presentar por su mal uso .

Es de gran importancia que las entidades de salud del sector público de Bogotá de acuerdo con sus organigramas, involucren no solamente a personal de tecnología para la implementación y divulgación de su plan de concienciación, sino que también incluyan a personal de áreas como: recursos humanos, control interno, calidad y del equipo de comunicaciones, brindándoles previamente formación y capacitación en seguridad de la información para de esta manera y a través de su apoyo, se pueda lograr generar una adecuada cultura en seguridad al interior de la organización en la que todos estén involucrados.

BIBLIOGRAFÍA

- AGUILAR, Mario; Pedagogía de la intencionalidad: educando para una conciencia activa. {En línea}. {consultado mayo 2020}. Disponible en: https://elibro-net.ucatolica.basesdedatosezproxy.com/es/lc/ucatolica/titulos/67099?as_all=conciencia&as_all_op=unaccent__icontains&prev=as&fs_page=3
- BANCO INTERAMERICANO DE DESARROLLO; ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Ciberseguridad: ¿estamos listos en América Latina y el Caribe? {En línea}. {Consultado marzo 2020}. Disponible en: https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean
- BIDDLE, Susan. Ciberseguridad en el sector de salud. {En línea}. {Consultado marzo 2020}. Disponible en: https://revistaempresarial.com/salud/salud-ocupacional/ciberseguridad-sector-salud/
- BOLETÍN OFICIAL DEL ESTADO. Reglamento (UE) 2016/679 del parlamento europeo y del concejo. {En línea}. {Consultado abril 2020}. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf
- CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. El Tictac presenta su informe: Tendencias del Cibercrimen en Colombia primer trimestre de 2020. {En línea}. {Consultado abril 2020}. Disponible en: https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/2019-2020/
- CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020. {En línea}. {Consultado abril 2020}. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/
- CASTRO CASTRO, Paola Andrea; MONROY SOSA, Valeria Alejandra. Guía estratégica para la sensibilización en seguridad de la información aplicada al laboratorio farmacéutico Expofarma S.A. {En línea}. {Consultado abril 2020}. Disponible en: http://polux.unipiloto.edu.co:8080/00002377.pdf
- CISCO. Defiéndase contra amenazas críticas de la actualidad. Reporte de Amenazas 2019. {En línea}. {Consultado abril 2020}. Disponible en: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/cybersecurity-series-threat.pdf
- COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien

jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.. Bogotá, 2009, no. 47.223.

- COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581. (17, octubre 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá, 2012, no. 48.587.
- COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 2015. (31, enero 2020). Por medio del cual se crea la historia clínica electrónica interoperable y se dictan otras disposiciones. Bogotá, 2020.
- COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 23. (18, febrero 1981). Por la cual se dictan normas de ética médica. Bogotá, 1981, no. 35.711. Art. 34.
- COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 594. (14, julio 2000). Por medio de la cual se dicta la ley general de archivos y se dictan otras disposiciones. Bogotá, 2000, no. 44.084.
- COLOMBIA. CONGRESO DE LA REPUBLICA. Resolución 839. (27, marzo 2017). Por la cual se modifica la resolución 1995 de 1999 y se dictan otras disposiciones. Bogotá, 2017.
- DIAZ ROMERO, Joseph Cristopher; PRIETO DURAN, Jhon Cesar. Sistema de gestión de la seguridad de la información para la proyección de los datos personales en el uso de historia clínica electrónica del hospital Rafael Uribe Uribe. {En línea}. {Consultado marzo 2020}. Disponible en: http://repository.udistrital.edu.co/handle/11349/22399
- EHCOS BY EVERYS HEALTH. Ciberseguridad en los hospitales: prevenir como defensa a cualquier ataque. {En línea}. {Consultado marzo 2020}. Disponible en: https://www.ehcos.com/ciberseguridad-hospitales-prevenir-como-defensa-ataque/#
- GUZMÁN SOLANO, Sandra Liliana. Guía para la implementación de la norma ISO 27032. {En línea}. {Consultado marzo 2020}. Disponible en: https://repository.ucatolica.edu.co/handle/10983/23385
- HOMELAND SECURITY. A life line: patient safety and cibersecurity. {En línea}. {Consultado marzo 2020}. www.dhs.gov/sites/default/files/publications/ia/ia_vulnerabilities-healthcare-it-systems.pdf
- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013.

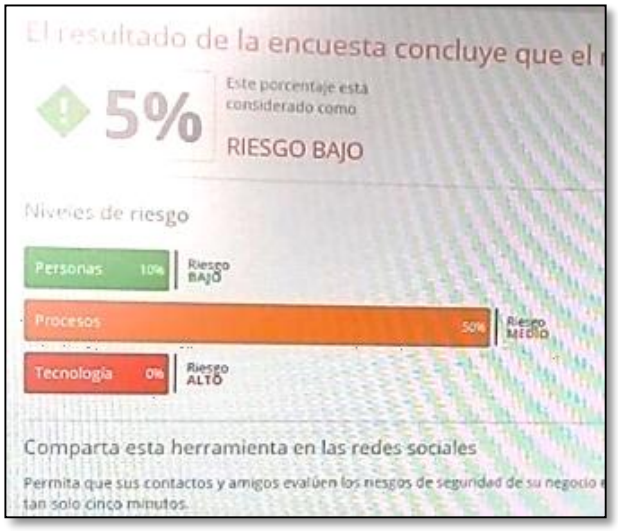
- INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). Políticas de seguridad para la pyme. Concienciación y Formación. {En línea}. {Consultado marzo 2020}. Disponible en: https://www.incibe.es/protege-tu-empresa/herramientas/politicas
- Instituto Nacional de Ciberseguridad (INCIBE). Kit de concienciación. {En línea}. {Consultado octubre 2020}. Disponible en: https://www.incibe.es/protege-tu-empresa/kit-concienciacion
- Instituto Nacional de Ciberseguridad (INCIBE). Formación. {En línea}. {Consultado octubre 2020}. Disponible en: https://www.incibe.es/protege-tu-empresa/formacion
- Instituto Nacional de Ciberseguridad (INCIBE). Desarrollar cultura en seguridad. {En línea}. {Consultado octubre 2020}. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad
- MINISTERIO DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES. Modelo de seguridad y privacidad de la información. {En línea}. {Consultado marzo 2020}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
- MINISTERIO DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES. Plan de capacitación, sensibilización y comunicación de Seguridad de la Información. {En línea}. {Consultado marzo 2020}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf
- MOLANO ESPINEL, Rafael Antonio. Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de TI para la empresa Market MIX. {En línea}. {Consultado marzo 2020}. Disponible en: https://repository.ucatolica.edu.co/handle/10983/15240
- NIST (National Institute of Standards and Technology). Wilson, Mark; Hash, Joan. Special Publication 800-50. Building and Information Technology Security Awareness and Training Program. {En línea}. {Consultado mayo 2020}. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-50/final
- RODRIGUEZ AREVALO, Javier Horacio. TORRES CALDERON, Wilmer Alfonso. Análisis de riesgos de seguridad de la información del área IT de la empresa Royal Services S.A. {En línea}. {Consultado marzo 2020}. Disponible en: https://repository.ucatolica.edu.co/handle/10983/23389

ANEXO 1. EVIDENCIA DE RESULTADOS HERRAMIENTA DE AUTODIAGNOSTICO INCIBE.

RESULTADO REFERENTE 1

RESULTADOS REFERENTE 2

RESULTADOS REFERENTE 3



ANEXO 2. ENCUESTA SEGURIDAD DE LA INFORMACIÓN ENTIDADES DE SALUD DEL SECTOR PÚBLICO DE BOGOTÁ.

La siguiente encuesta tiene como objetivo evaluar el conocimiento que tiene el encuestado respecto a la seguridad de la información que se maneja actualmente en la organización para la cual trabaja. Por favor sea lo mas sincero posible en sus respuestas, ya que de acuerdo con los resultados obtenidos se podrá realizar un análisis respecto a las posibles falencias que se puedan estar presentando.

1. ¿Conoce usted la Política de Seguridad de la Información implementada en la entidad de salud para la cual trabaja?

   Si

   No

2. ¿Conoce usted la diferencia entre información Pública, privada, confidencial y sensible?

   Si

   No

3. ¿Sabe usted si en la entidad de salud para la cual trabaja existe una política relacionada con la clasificación de la información (pública, privada, confidencial, sensible)?

   Si

   No

4. ¿Sabe usted si en la entidad de salud para la cual trabaja se tienen establecidos acuerdos de confidencialidad en cuanto al manejo de información por parte de los funcionarios?

   Si

   No

5. ¿Conoce usted las consecuencias legales a las cuales se encuentra expuesto por el incumplimiento de alguno de los puntos establecidos en la Política de Seguridad de la Información establecida por la organización para la cual trabaja?

   Si

   No

6. ¿Ha recibido alguna capacitación sobre seguridad de la información para la entidad para la cual trabaja?

   Si

   No

7. ¿Cuántas veces al año recibe capacitación sobre seguridad de la información?

   a) Una vez al año.
   b) Dos veces al año.
   c) Más de dos veces al año.
   d) No recibe capacitación al respecto.

8. ¿Quién es el responsable de instalar y mantener el software de seguridad en su computadora?

   a) Empleados (Usted).
   b) Personal del área de TI.

9. ¿Qué versión de Windows está instalada en el equipo sobre el que a diario desempeña sus labores?

    a) Windows 10
    b) Windows 8
    c) Windows 8.1
    d) Windows 7
    e) Windows Vista
    f) Windows XP
    g) No sabe

10. ¿Tiene su equipo de cómputo empresarial instalado un software Antivirus?

    Si

    No

    No sabe

11. ¿Sabe usted que es ingeniería Social?

    Si

    No

12. ¿Conoce usted si la entidad para la cual trabaja ha sufrido ataques informáticos durante el último año?

    Si

    No

    No sabe

13. ¿Conoce usted los riesgos a los que está expuesta la información de las historias clínicas en caso de que la misma sea mal utilizada?
    Si
    No

14. ¿Conoce usted los requerimientos mínimos para el adecuado manejo de las historias clínicas dentro de la entidad?
    Si
    No

15. ¿Conoce usted los parámetros mínimos definidos por la organización para establecer sus contraseñas?
    Si
    No

16. ¿Alguna vez ha utilizado su correo corporativo para enviar información a alguna cuenta personal?
    Si
    No

17. ¿Cuándo envía un correo electrónico se asegura de que la información adjunta este cifrada?
    Si
    No

18. ¿Utiliza su dispositivo móvil para desempeñar algunas de las tareas que tiene bajo su cargo?
    Si
    No

19. ¿En algún momento ha tenido que utilizar su computador personal para desempeñar tareas relacionadas con su trabajo?
    Si
    No

20. ¿Alguna vez ha compartido su contraseña con alguno de sus compañeros de trabajo?
    Si
    No

21. ¿Conoce las diferentes tipos de ataques informáticos a los que está expuesta la información de las organizaciones?
    Si
    No

ANEXO 3. PLAN DE CONCIENCIACIÓN

PLAN CONCIENCIA.

IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DE SALUD DEL SECTOR PÚBLICO DE BOGOTÁ.

PRESENTADO POR: FABIO MARTINEZ OSORIO

ÍNDICE

IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DE SALUD DEL SECTOR PÚBLICO DE BOGOTA.

IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DE SALUD DEL SECTOR PÚBLICO DE BOGOTA.

1. Introducción.

Actualmente y según la experiencia se ha ido demostrando que los más grandes errores de seguridad de la información resultan en torno a los descuidos que las personas presentan en el desarrollo de sus actividades diarias, catalogándolos así como uno de los eslabones más importantes pero también más débiles de la cadena de la seguridad dentro de una organización.

En el momento de garantizar la seguridad de una organización sin importar su naturaleza, además de contar con una infraestructura robusta, políticas, normas, procesos, procedimientos y la formación del personal encargado, la Dirección se debe asegurar de que se incluya a todos los empleados y que los mismos, sean conscientes de la importancia que tienen de la información que manejan.

Para lograrlo, se hace necesario emprender acciones de concienciación que sirvan para dar a conocer a los empleados el cómo aplicar aspectos importantes relacionados con la seguridad de la información en el desempeño cotidiano de sus funciones. En consecuencia, es necesario que los empleados reconozcan las amenazas y los riesgos a los que se encuentran expuestos, para que tengan la habilidad de reaccionar correctamente ante posibles situaciones que los puedan afectar a ellos y a la organización en general, contribuyendo así a la creación de una cultura en seguridad de la información y al fortalecimiento de su modelo y estrategia de negocio.

2. Antecedentes generales.

Durante los últimos años son múltiples los ataques informáticos que han sufrido las entidades del sector salud a nivel mundial, por lo que cabe destacar como ejemplo algunos de los casos y las consecuencias que estos han generado. Estos casos son:

I. El ataque de ransomware WannaCry en mayo de 2017, que afectó a más de 300.000 máquinas en 150 países, apuntando a sistemas operativos de Windows desactualizados. Dicho ataque se extendió por países de Europa y Asia, incluido Reino Unido, donde los hospitales se vieron obligados a desviar a los pacientes después de que el malware impidiera que los médicos accedieran a los registros médicos retrasando así la atención normal de los pacientes y provocando la cancelación de operaciones y otras citas de alta complejidad.[13]

II. Un ataque de ransomware al Hospital Universitario de Dusseldorf (Alemania) colapsó el servicio de urgencias del centro, que tuvo que cerrar temporalmente la sala de urgencias y, como resultado de ello, una paciente gravemente enferma falleció mientras era trasladada a otro hospital.[14]

III. Información personal de 2’373.764 pacientes mexicanos que forman parte de una base de datos de una compañía de telemedicina están disponibles de forma pública como consecuencia de la mala configuración de una base de datos MongoDB.

IV. Las violaciones de datos y los ataques de ransomware que sufrieron en 2019 las organizaciones de salud de los Estados Unidos representaron un costó al sector estimado en $ 4 mil millones de dólares. Cinco organizaciones de atención médica de dicho país informaron ataques de ransomware en una sola semana, lo que provocó que, por ejemplo, un centro de prácticas médicas en el estado de Michigan cerrara después de negarse a pagar un rescate a los atacantes.[15]

---

[13] https://www.fiercehealthcare.com/privacy-security/ransomware-attack-shuts-down-nhs-hospitals-as-malware-spreads-across-12-countries

[14] https://www.elmundo.es/internacional/2020/09/18/5f647ae0fc6c83241c8b4663.html

[15] https://www.welivesecurity.com/la-es/2020/04/22/por-que-hospitales-blanco-atractivo-cibercriminales/

V. Ataque informático del que fue víctima el Hospital San Juan de Dios en Armenia en abril del 2018 y en el cual se encripto información del servidor principal (información por la que ciberdelincuentes pedían pagar un rescate) como ocurre en todos los casos o en el caso de la Subred Sur de Salud de Bogotá sobre la cual se denunció un robo cibernético por valor de 1.500 millones de pesos el 6 de agosto de 2018.

3. Objetivo.

Garantizar que los funcionarios de las entidades de salud del sector público de Bogotá conozcan, interioricen y cumplan los diferentes lineamientos establecidos por la organización respecto a la seguridad de la información que manejan en su día a día, advirtiéndoles de los riesgos a los que se exponen por un mal uso de los dispositivos y soluciones tecnológicas a su disposición.

4. Alcance.

El presente plan aplica para todo el personal vinculado a las entidades de salud del sector público de Bogotá, es decir funcionarios y contratistas, así como para las partes interesadas.

5. Usuarios y necesidades.

De acuerdo con el estudio realizado previamente, el presente plan está enfocado a funcionarios y contratistas de salud del sector público quienes deben conocer todos los lineamientos de seguridad de la información de la entidad y las reglas de comportamiento adecuados para proteger tanto los sistemas como la información institucional que tienen a su cargo.

6. Estrategia de aplicación del plan de concienciación.

La estrategia que se sugiere para la aplicación del presente plan de concienciación está basada en el uso de escenarios reales en donde se involucre a los funcionarios y contratistas en ataques dirigidos previamente definidos y diseñados por los encargados del Área de Sistemas de Información TIC, quienes una vez obtengan los resultados puedan implementar junto con las áreas de: (Recursos Humanos, Gestión del conocimiento, Control Interno, Calidad y Comunicaciones de las entidades) los respectivos recursos de apoyo como:

- Planes de formación y capacitación (presenciales o virtuales).
- Folletos informativos (físicos o digitales).
- Carteles de publicidad dispuestos en lugares estratégicos dentro de la entidad que capten la atención de los funcionarios.
- Creación de día alusivo a la Seguridad de la Información.

- Uso de plataformas tecnológicas (Intranet, plataformas de e-learning, videos, gamificación (aprendizaje a través de juegos), etc.)
- Otros.

7. Temas clave a concienciar.

- **Difusión de la Política de Seguridad de la Información de la entidad.**

  El propósito de socializar la política de seguridad de la información ayudará a que sus funcionarios y demás partes interesadas estén alineados con la estrategia de seguridad de su negocio ayudando a cumplir los objetivos para los que la misma fue definida y así mismo conozcan las diferentes sanciones asociadas por su incumplimiento.

- **Planes de Capacitación en Seguridad de la Información.**

  El propósito de implementar planes de capacitación en Seguridad de la Información ayudará a que sus funcionarios y partes interesadas cuenten con la educación y formación apropiada y actualizada de acuerdo con sus roles y perfiles dentro de la organización y así mismo, conozcan los riesgos a los cuales se encuentran expuestos.

- **Identificación de ataques informáticos.**

  El propósito de conocer y poder identificar los diferentes tipos de ataques informáticos a los cuales se exponen los sistemas de información en la actualidad ayuda a mitigar el riesgo de que su organización se vea afectada por el impacto que podría provocar la materialización de un ciberataque.

- **Ingeniería Social.**

  El propósito de conocer las diferentes técnicas de ingeniería social le permitirá a sus funcionarios actuar de manera responsable en el desarrollo de sus actividades evitando ser víctimas de delincuentes informáticos.

- **Gestión de contraseñas.**

  El propósito de conocer la importancia de una adecuada gestión de contraseñas le permitirá proteger la confidencialidad, integridad y

disponibilidad de toda la información que se maneja frente a posibles ataques o abusos de personal interno o externo dentro de su organización.

- **Uso seguro de correo electrónico.**

  El propósito de conocer la importancia del uso seguro del correo electrónico al interior de su organización le permitirá garantizar que este no sea un medio de filtrado o robo de información importante que afecte no solo la confidencialidad de la información que maneja la entidad, sino también su buen nombre y reputación.

- **Seguridad en dispositivos móviles.**

  El propósito de conocer la importancia que tiene la seguridad en dispositivos móviles le permitirá tomar las precauciones necesarias para que este tipo de activos no representen una brecha de seguridad que pueda ser utilizada por delincuentes informáticos para afectar la seguridad de la información de su organización.